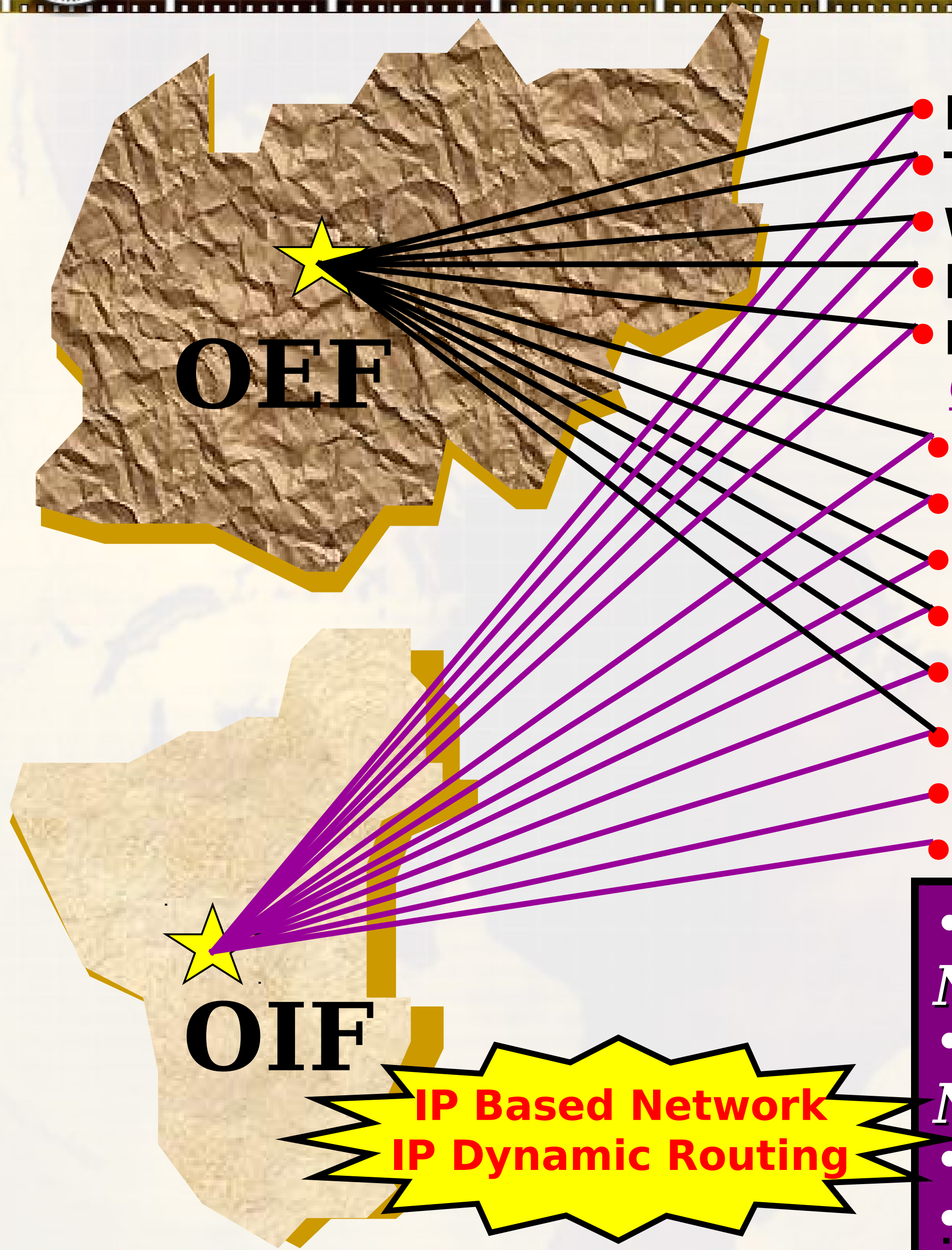
PACOM 2004 Information Assurance Confere

Army Network Transformation and Information Assurance

LTG Steven W. Boutelle
Army CIO/G-6

26 May 2004

Warfighting in 2003/4 and Beyond



IP Based Network
IP Dynamic Routing

Operating Environment

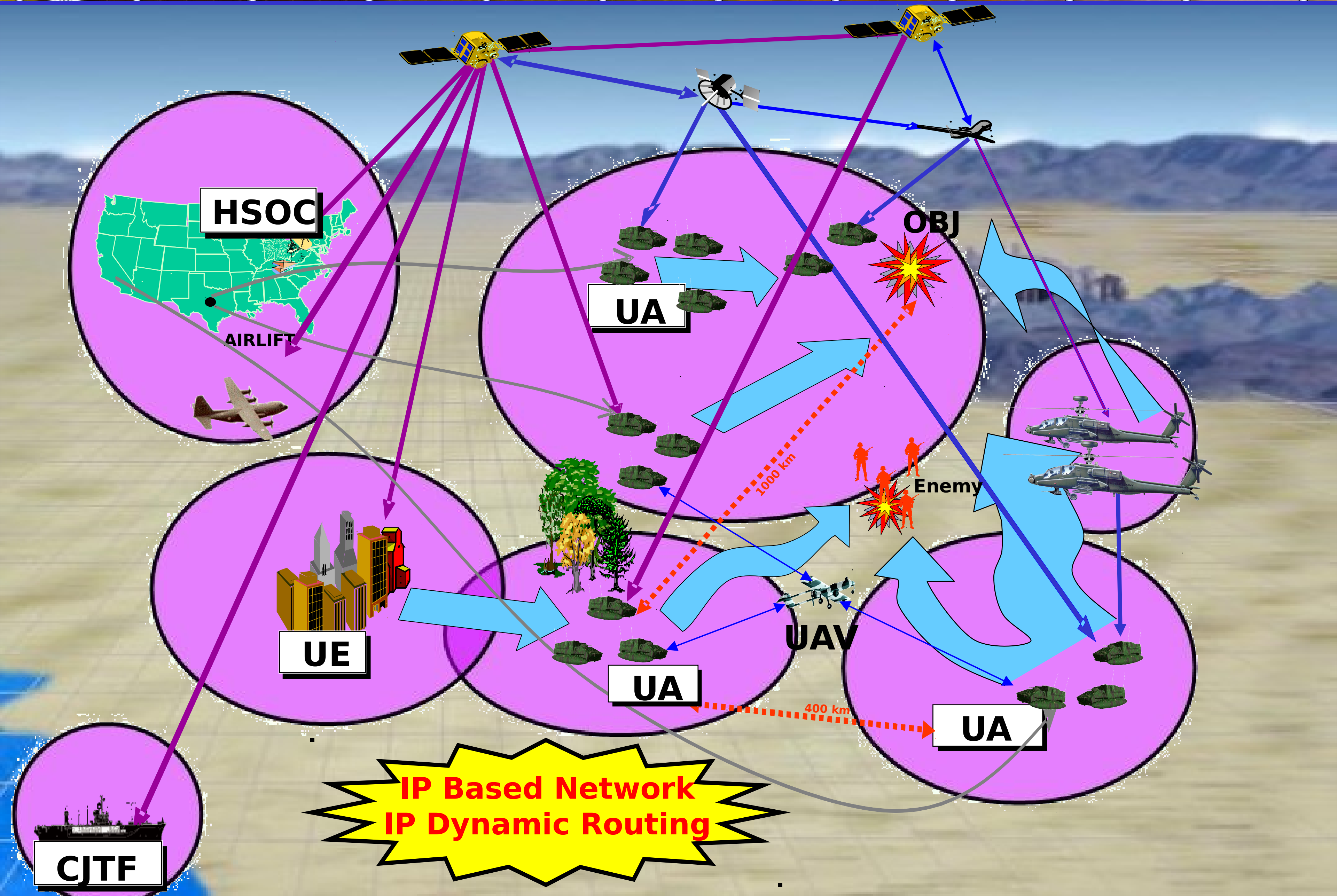
- Non-Doctrinal Command Relations
- Task Organized Signal Support
- Widely dispersed C2 Locations
- High Operational Tempo
- Large Operational Environment

Communications Environment

- NIPRNet, SIPRNet, VTC, Red Phon
- Non-LOS
- Connected to the GIG
- Joint/Coalition, Conventional/SOF
- Stability Force Communications
- Blue Force Tracking
- OTM Networking
- Wireless TOCS

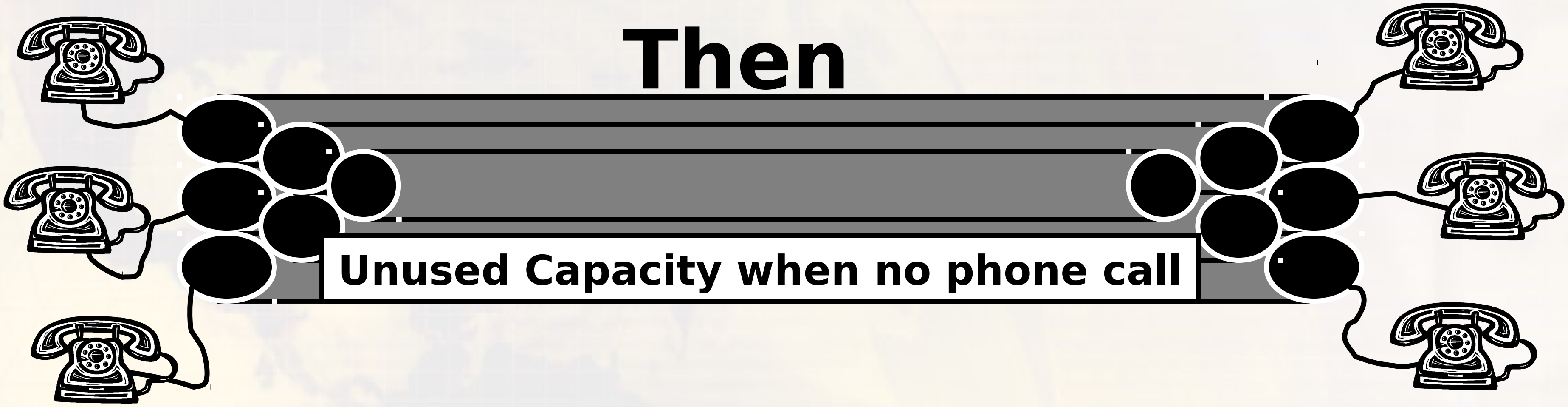
- ***Joint/Coalition Networking***
- ***OTM/OTQH/Sanctuary Networks***
- ***Part of the GIG***
- ***Joint SA***

LandWarNet – FY20XX



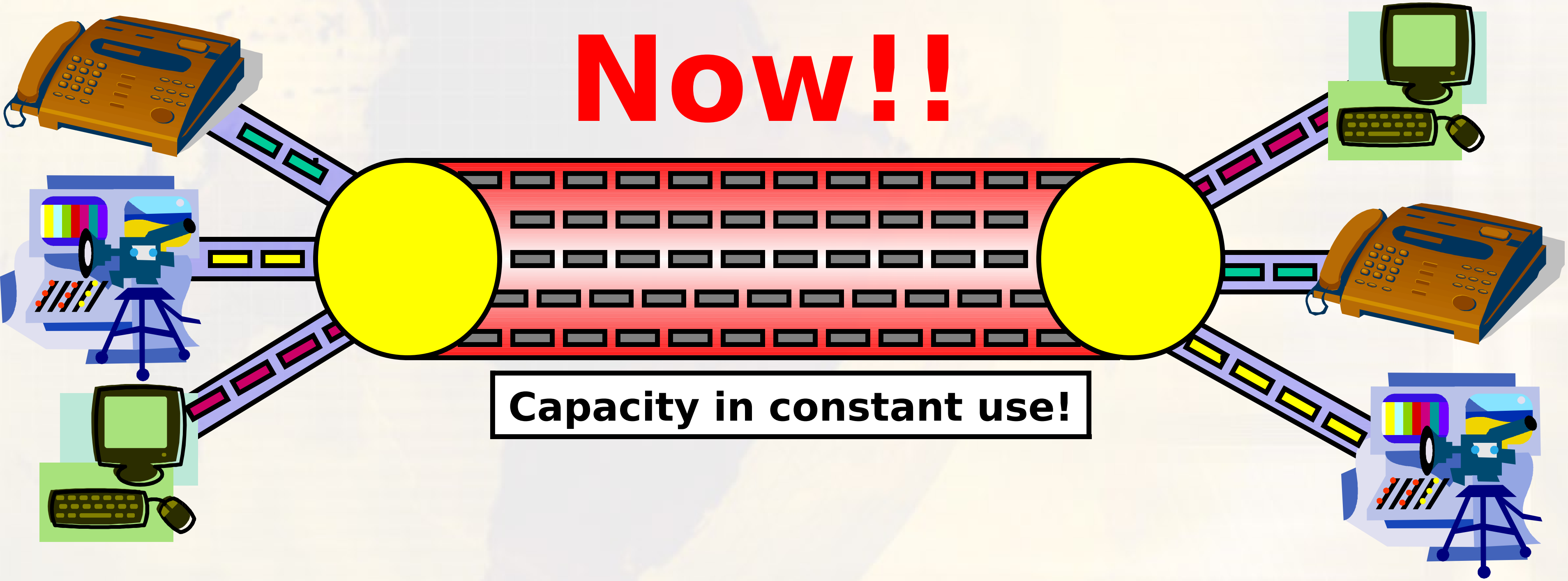
The Network: Then and Now

Then



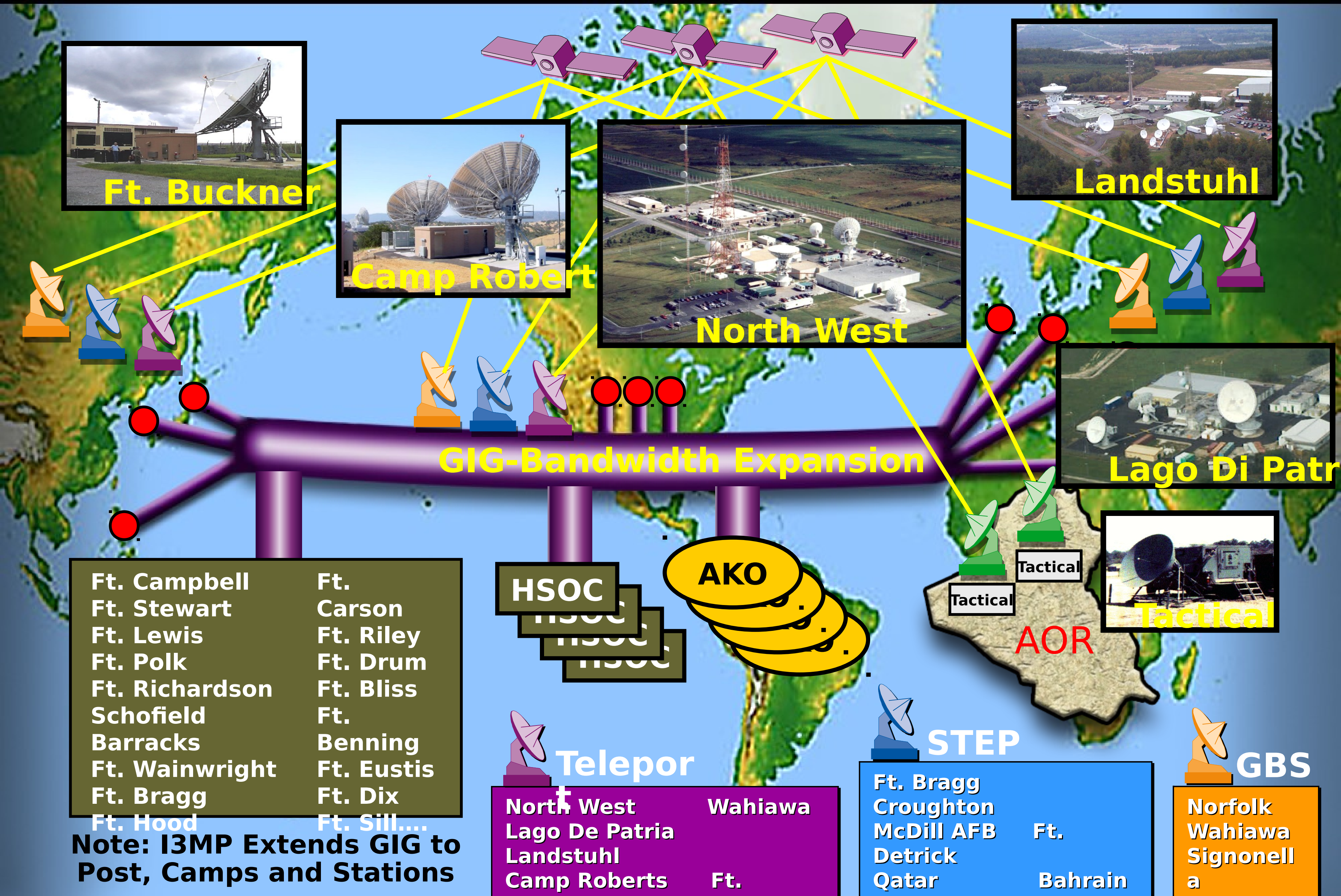
Unused Capacity when no phone call

Now!!



Capacity in constant use!

DISN (GIG-BE) 2004 - 2007



Ft. Campbell
Ft. Stewart
Ft. Lewis
Ft. Polk
Ft. Richardson
Schofield Barracks
Ft. Wainwright
Ft. Bragg
Ft. Hood

Ft. Carson
Ft. Riley
Ft. Drum
Ft. Bliss
Ft. Benning
Ft. Eustis
Ft. Dix
Ft. Sill....

Note: I3MP Extends GIG to Post, Camps and Stations

North West
Lago De Patria
Landstuhl
Camp Roberts

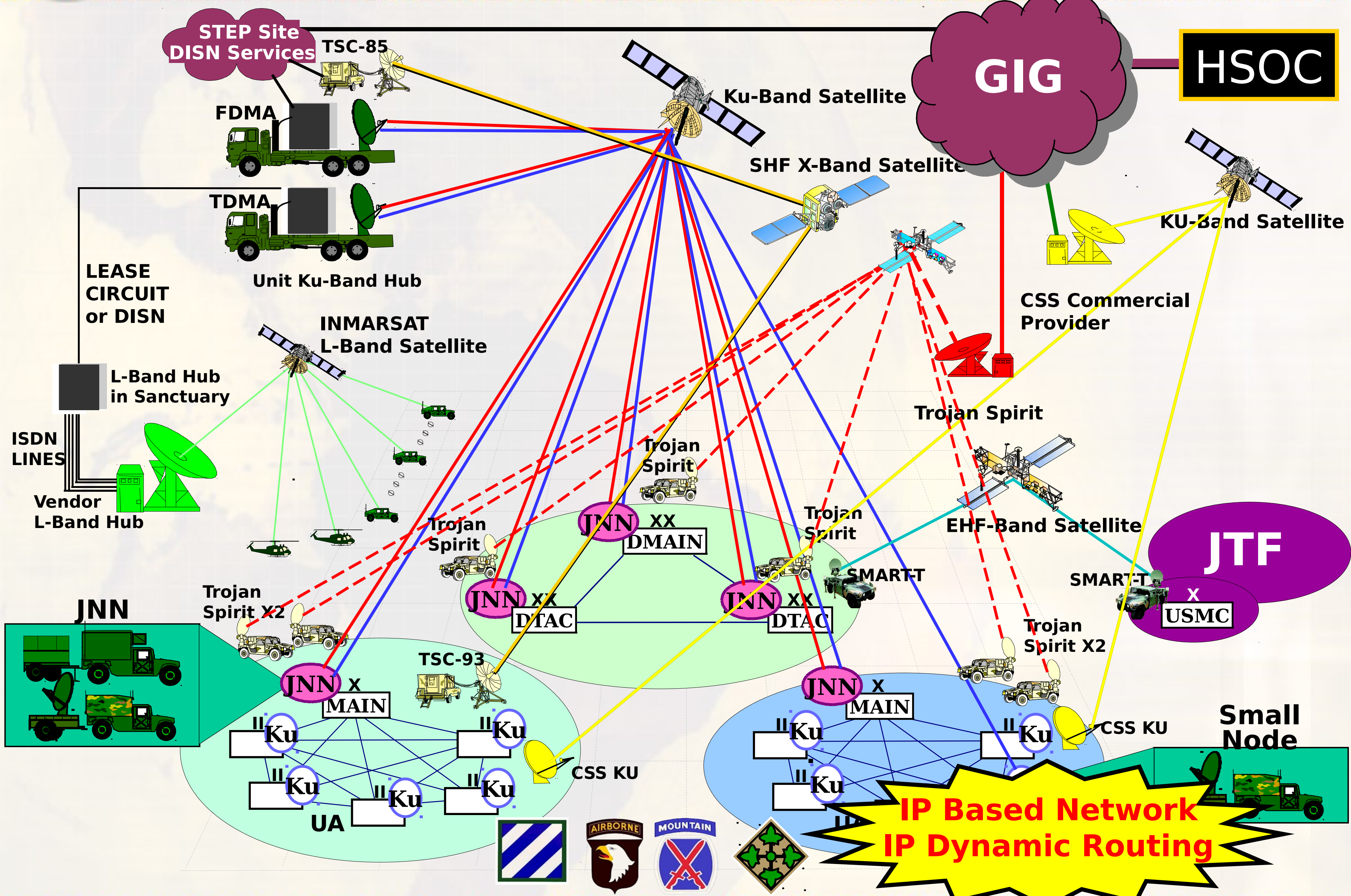
Wahiawa
Ft.

Ft. Bragg
Croughton
McDill AFB
Detrick
Qatar

Ft.
Bahrain

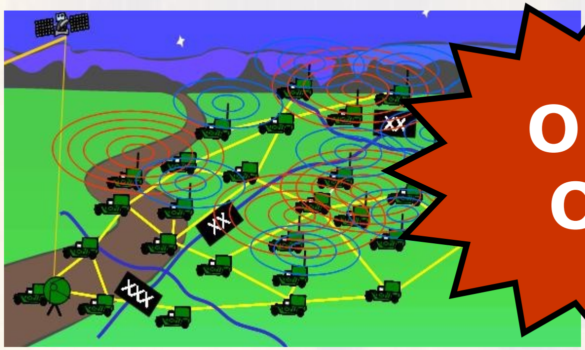
Norfolk
Wahiawa
Signonell
a

Technical Approach For 3ID....



Current, Interim and Future Capabilities

MSE/TRI-TAC

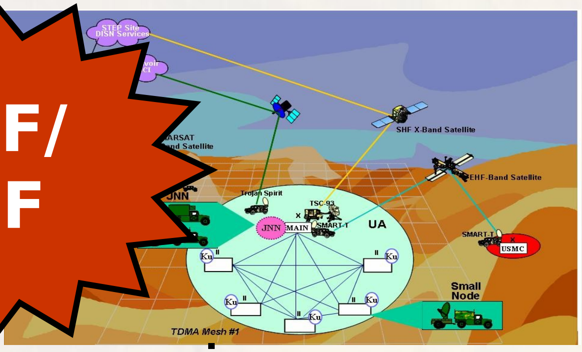


OEF/
OIF

d-War Linear Battlefield Smaller Area of Operations

- Only Network Management (NM) Capability
- Limited Mobility
- Large transportation requirements
- Manpower intensive
- TROJAN Spirit and other Stove Pipe systems supplement network

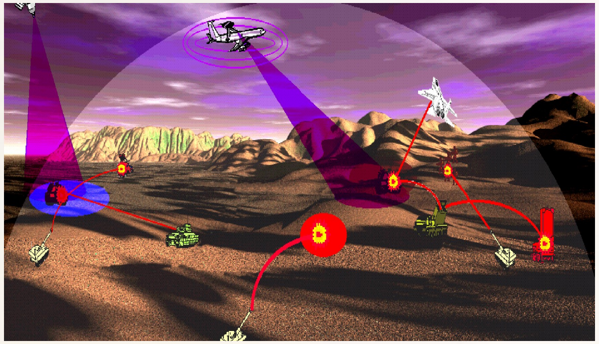
INTERIM



Linear/Non-linear Battlefield Area of Operations

- Migrate towards an IP based network
- Increased NLOS transmission systems
- IP capability (data+voice) at Division, Brigade and Battalion CPs
- Joint/Coalition/Current MSE interface provided through Joint Network Node
- SIPR/NIPR/Coalition service at Bde/Division CPs
- SIPR Voice/Digital service only at all Bn CPs

WIN-T



Non-linear Battlefield Expanded Area of Operations

- Full NETOPS Capability (Net Management, (IA, IDM) to include Speed of Service and QOS
- On the Move Communications
- Network Services integrated and embedded Within Warfighting Platforms
- Optimal use of manpower utilizing automated Services
- Fully integrates all systems to make one Network (Net-Centric)

Adjusting the Acquisition Strategy

Threats

are are real, non-traditional and highly diversified”

- Defense Science Board

Internal:

Known and unknown “back doors”

“Stand-alone” Networks -

Insider misconduct -

Software Vulnerabilities -

Misconfiguration -

External:

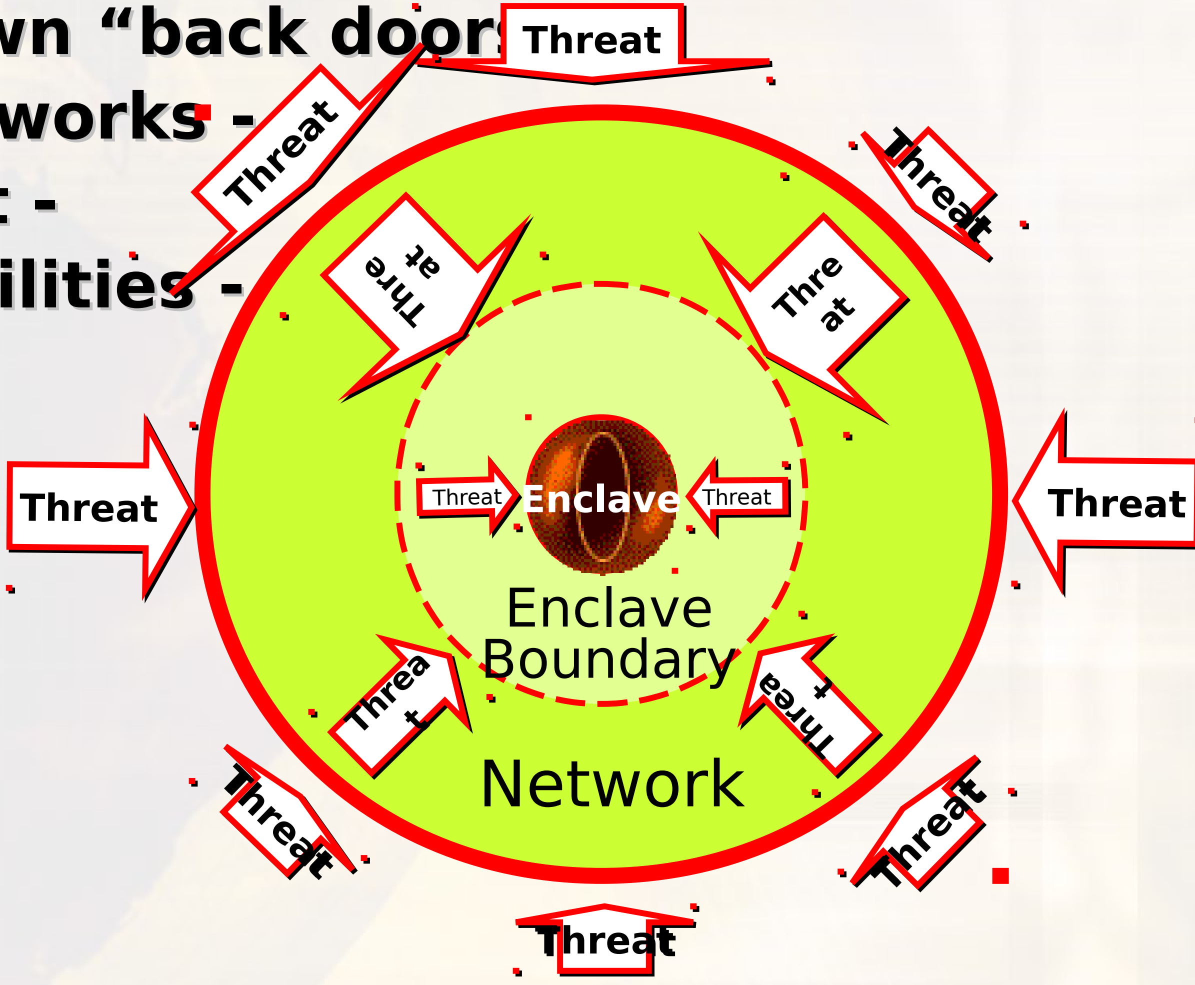
Worms -

Viruses -

Hackers -

Denial of Service -

Cyber Warfare -



Cyber Threat Reporting

An incident may involve one site or hundreds (or even thousands) of sites. Also, some incidents may involve ongoing activity for long periods of time. – ***CERT CC***

Incidents are Defined as hackers, viruses, worms, denial of service attacks, etc.

Number of incidents reported 1988-1989

Year	**1988**	**1989**
Incidents	**6**	**132**

1990-1999

Year	**1990**	**1991**	**1992**	**1993**	**1994**	**1995**	**1996**	**1997**	**1998**	**1999**
Incidents	**252**	**406**	**773**	**1,334**	**2,340**	**2,412**	**2,573**	**2,134**	**3,734**	**9,859**

2000-2003

Year	**2000**	**2001**	**2002**	**2003**
Incidents	**21,756**	**52,658**	**82,094**	**137,529**

Total incidents reported to CERT CC (1988-2003): 319,992

HackerWatch.org

Event Tracking:

Significant incidents recently reported

24 Hours	**78,541,667**
7 Days	**547,791,660**
30 Days	**2,356,379,55**

* As of 20 May

The Threat is Growing

Global Terrorist Incidents

1968-1997 = 8509 (20 Years)

1997-2004 = 9024 (6+ Years)

- **Al Qaida Islamic Jihad**
- **Hamas**
- **Hisbollah**
- **Palestine Liberation Front**
- **Etc., Etc.**
- ***Trained and Educated – Phd's, Engineers, Technicians***
- ***Highly D***

Threat Level = HIGH

OCT 23, 1983
Marine Barracks
242 Marines killed

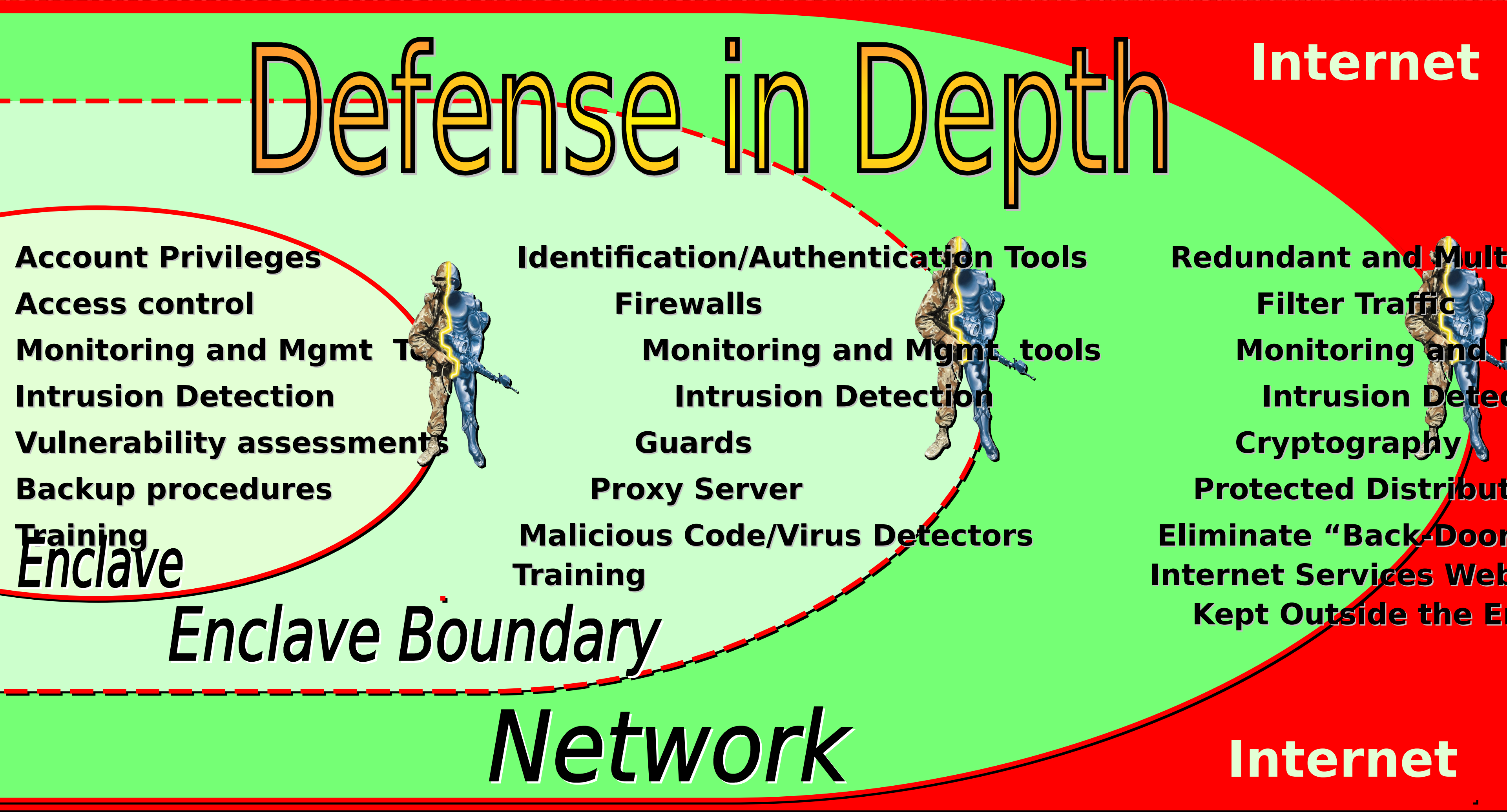
Aug 7 1998
U.S. Embassies In East Africa
54 killed
5000 Injured

Oct 12, 2000
USS Cole
17 Sailors killed
39 Injured

Sept 11, 2001
WTC/Pentagon
3000+ killed,
thousands more

4630+ Terrorist Attacks Worldwide Since

Defending our Networks



Defense in Depth

Internet

Account Privileges
Access control
Monitoring and Mgmt To
Intrusion Detection
Vulnerability assessments
Backup procedures
Training

Enclave

Identification/Authentication Tools
Firewalls
Monitoring and Mgmt tools
Intrusion Detection
Guards
Proxy Server
Malicious Code/Virus Detectors
Training

Enclave Boundary

Redundant and Mult
Filter Traffic
Monitoring and M
Intrusion Detec
Cryptography
Protected Distribut
Eliminate “Back-Door
Internet Services Web
Kept Outside the E

Network

Internet

Net-Centric Defense

- ***One Virtual Network***
- ***NETCOM- Single Network Defender/Manager***
- ***Robust Network Design and***

Take Away's

- Army Networks Are Moving to IP Based Architecture
- Interim Warfighter Network and WIN-T – IP based networks at the tactical level
- Threats are always out there *and growing* – sophisticated enemies
- Information Assurance – Crucial today, more so in the future

Questions?

Provide Relevant and Ready Land Power Capability to the Combatant Commander as